CLAIMS

What is claimed is:

1. A random number generator comprising:

a plurality of cross-connected latches providing at least two latch outputs;

at least one input of one latch of the plurality of latches being driven by a clock signal;

a first XOR that receives the at least two latch outputs as an input;

wherein said first XOR generates a mistake signal "E" when its inputs do not match from the at least two latch outputs being at different logic states; and

wherein the mistake signal is compared with a previously stored mistake signal by a second XOR to determine whether to obtain a random bit from a pseudo random stream of bits.

2. The random number generator according to claim 1, further comprising:

an exclusive or network comprising a plurality of strings of cascaded flip-flops, wherein an output of each of the plurality of strings is connected to the first XOR circuit, and wherein each respective latch output of the at least two latch outputs is connected to an input of a respective string of the plurality of cascaded flip-flops.

3. The random number generator according to claim 2, wherein the plurality of strings of cascaded flip flops comprise D flip-flops.

4. The random number generator according to claim 2, further comprising a flip-flop arrangement driven by a third XOR to provide an acquisition signal "A" that is input to the XOR network by providing a clock input to the strings of cascaded flip-flops.

5. The random generator according to claim 1, wherein a logical value of said previously stored mistake is stored in a flip-flop.

6. The random generator according to claim 1, wherein if the previously stored mistake disagrees with the mistake "E" then a bit is stored in a shift register.

7. The random generator according to claim 5, wherein if the previously stored mistake disagrees with the mistake "E" then a bit is stored in a shift register.

8. The random number generator according to claim 7, wherein the bit is stored in the shift register when the previously stored value is a logical zero.

9. The random number generator according to claim 7, wherein the shift register is enabled for shifting via an AND gate, wherein said AND gate has a first input from said second XOR and a second input from said flip-flop.

10. The random number generator according to claim 1, wherein the random bit obtained from the pseudo-random stream of bits is generated by a Linear Feedback Shift Register (LFSR).

11. The random number generator according to claim 10, wherein the LFSR has at least 64 bits.

12. The random number generator according to claim 7, wherein the random bit obtained from the pseudo-random stream of bits is generated by a Linear Feedback Shift Register (LFSR).

13. The random number generator according to claim 12, wherein the LFSR has at least 64 bits.

14. A method of random number generation comprising the steps of:

(a) providing a plurality of cross-connected latches having at least two latch outputs;

(b) driving at least one input of one latch of the plurality of latches by a clock signal;

(c) connecting a first XOR that receives the at least two latch outputs as an input;

(i) wherein said first XOR generates a mistake signal "E" when its inputs do not match from the at least two latch outputs(latch0, latch1) being at different logic states; and

(ii) comparing the mistake signal with a previously stored mistake signal by a second XOR to determine whether to obtain a random bit from a pseudo random stream of bits.

15. The method according to claim 14, wherein step (c) further comprises:

(iii) obtaining the random bit from the pseudo-random stream of bits.

The method according to claim 14, further comprising:

providing an exclusive or network comprising a plurality of strings of cascaded flip-flops, wherein an output of each of the plurality of strings is connected to the first XOR circuit, and wherein each respective latch output of the at least two latch outputs is connected to an input of a respective string of the plurality of cascaded flip-flops.

The method according to claim 16, wherein the plurality of strings of cascaded flip flops comprise D flip-flops.

18. The method to claim 16, further comprising providing a flip-flop arrangement driven by a third XOR to provide an acquisition signal "A" that is input to the XOR network by providing a clock input to the strings of cascaded flip-flops.

19. The method according to claim 14, wherein a logical value of said previously stored mistake is stored in a flip-flop.

20. The method according to claim 14, wherein if the previously stored mistake disagrees with the mistake "E" then a bit is stored in a shift register.

21. The method according to claim 19, wherein if the previously stored mistake disagrees with the mistake "E" then a bit is stored in a shift register.

22. The method according to claim 21, wherein the bit is stored in the shift register only when the previously stored value is a logical zero.

23. The method according to claim 21, wherein the shift register is enabled for shifting via an AND gate, wherein said AND gate has a first input from said second XOR and a second input from said flip-flop.